

殯葬服務業個人資料檔案安全維護管理辦法

條 文	說 明
第一條 本辦法依個人資料保護法（以下簡稱本法）第二十七條第三項規定訂定之。	明定本辦法之法源依據。
第二條 本辦法所稱主管機關，在中央為內政部；在直轄市為直轄市政府；在縣（市）為縣（市）政府。	明定本辦法所稱各級主管機關。
第三條 殯葬服務業應訂定個人資料檔案安全維護計畫（以下簡稱計畫），以落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 前項所稱殯葬服務業，指依殯葬管理條例第四十二條規定經直轄市或縣（市）主管機關許可經營之殯葬設施經營業及殯葬禮儀服務業。	一、第一項明定殯葬服務業應訂定個人資料檔案安全維護計畫，以建立相關管理機制並落實執行。 二、第二項明定本辦法適用對象。
第四條 殯葬服務業訂定計畫時，得視其規模、特性、保有個人資料之性質及數量等事項，參酌第六條至第二十條規定，訂定適當之安全維護管理措施。 前項計畫內容應包括下列項目，第二款相關項目必要時得整併之： 一、殯葬服務業之組織規模。 二、個人資料檔案之安全維護管理措施： （一）配置管理之人員及相當資源。 （二）界定蒐集、處理及利用個人資料之範圍。 （三）個人資料之風險評估及管理機制。 （四）事故之預防、通報及應變機制。 （五）個人資料蒐集、處理及利用之內部管理程序。 （六）設備安全管理、資料安全管理及人員管理措施。 （七）認知宣導及教育訓練。 （八）資料安全稽核機制。 （九）使用紀錄、軌跡資料及證據保存。 （十）個人資料安全維護之整體持續改善。 （十一）業務終止後之個人資料處理方法。 殯葬服務業應將計畫公告於營業處所適當之處，如有網站者，並揭露於網站	一、鑑於殯葬服務業規模不一，經營主體與型態未盡相同，尚難作統一規範，爰參照本法施行細則第十二條第二項規定意旨，第一項明定殯葬服務業得審酌其規模、特性、保有個人資料之性質、方法及數量等事項，訂定適宜並符合比例原則之安全維護管理措施。 二、考量國內殯葬服務業為數眾多，為利業者訂定計畫有所依憑，第二項明定殯葬服務業訂定計畫時應包括之內容項目，但保留彈性空間，業者得依個別情況自行斟酌整併相關項目。 三、為能讓全體員工明瞭個人資料保護之重要性，第三項明定殯葬服務業應將計畫公告於營業處所適當之處，以供所屬人員遵循，更可使當事人知曉業者保護個人資料之規定與作法，俾保護自身權益。

首頁，使其所屬人員及資料當事人均能知悉；計畫修正時，亦同。	
第五條 殯葬服務業應於直轄市、縣（市）主管機關許可經營之日起六個月內將計畫報請該直轄市、縣（市）主管機關備查；本辦法施行前已經許可經營殯葬服務業，應於本辦法施行之日起六個月內將計畫報請備查。 殯葬服務業應參酌計畫執行狀況、技術發展及相關法令修正等因素，檢視所定計畫是否合宜，必要時應予以修正，修正後應於十五日內將修正計畫報請備查。	為讓各直轄市、縣（市）殯葬主管機關能明瞭各殯葬服務業是否訂定個人資料檔案安全維護計畫，爰規定殯葬服務業應依營業項目為殯葬禮儀服務業或殯葬設施經營業，分別將計畫報請公司所在地或設施所在地之直轄市、縣（市）主管機關備查；如計畫有修正情形，亦應報請備查。
第六條 殯葬服務業應配置適當管理人員及相當資源，負責規劃、訂定、修正與執行計畫或業務終止後個人資料處理方法等相關事項。	為確保個人資料維護安全措施發生效能，爰規定殯葬服務業應配置適當管理人員及相當資源，負責該計畫或業務終止後個人資料處理方法之規劃、訂定、修正與執行等事宜。
第七條 殯葬服務業應確認蒐集個人資料之特定目的，依特定目的之必要性，界定所蒐集、處理及利用個人資料之類別或範圍，並定期清查所保有之個人資料現況。 殯葬服務業經清查發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期限屆滿而無保存必要者，應予刪除、銷毀或其他停止蒐集、處理或利用等適當之處置，並留存相關紀錄。	一、殯葬服務業依據本法施行細則第十二條第二項之規定，於安全維護計畫中得就個人資料範圍相關事項加以界定，並以與所欲達成之個人資料保護目的間有適當比例，爰明定殯葬服務業應界定其蒐集之特定目的為何，所蒐集之個人資料類別及範圍是否屬於必要。確認界定性質後，應定期清查所蒐集保有之個人資料是否符合所界定之範圍。 二、殯葬服務業在清查所蒐集之個人資料類別及範圍時，如發現有非本法第六條第一項規定且非屬特定目的之個人資料時，應予刪除或銷毀等適當之處置；如蒐集之特定目的消失或期限屆滿時，除因執行職務或業務所必須或經當事人書面同意者外，應依本法第十一條規定辦理，前開處置並應留存相關紀錄。
第八條 殯葬服務業依殯葬管理條例第五十六條規定委託代為銷售生前殯葬服務契約、墓基及骨灰（骸）存放單位之公司或商業，為執行業務所蒐集、處理或利用之個人資料視為該殯葬服務業所持有，於蒐集、處理或利用時應檢視是否符合特定目的之必要範圍，並接受該殯葬服務業監督。	一、第一項明定殯葬服務業與受委託之公司或商業間，無論係基於何種法律關係，其所蒐集、處理或利用之個人資料均應視為該業者所蒐集持有，須納入所訂定計畫之規範，接受該殯葬服務業監督，第二項明定相關監督事項。

前項監督措施應包含下列事項： 一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 二、受託者就第四條第二項採取之措施。 三、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。 四、委託機關如對受託者有保留指示者，其保留指示之事項。 五、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。 第一項受委託之公司或商業應遵行之個人資料安全維護管理事項及委託業務終止後，其蒐集、處理或利用持有個人資料檔案之處置方式，殯葬服務業應於委託契約明定之。	二、第三項規定殯葬服務業與其委託之公司或商業，應於委託契約明定受託者應遵行之個人資料安全維護管理事項及委託業務終止後，其持有個人資料檔案之處置方式。
第九條 殯葬服務業應依已界定蒐集、處理與利用個人資料之範圍及流程，分析評估可能發生之風險，並根據風險分析結果，訂定適當之管控措施。	明定殯葬服務業應參酌整體業務運作狀況，就第四條已界定蒐集、處理及利用個人資料之範圍與流程，分析評估可能發生之風險，並針對該可能發生之風險，採取必要之防範與管控措施。
第十條 殯葬服務業於蒐集個人資料應遵守本法第八條及第九條有關告知義務之規定，並區分個人資料屬直接蒐集或間接蒐集，分別訂定告知方式、內容及注意事項，要求所屬人員確實辦理。	依本法第八條及第九條規定，明定殯葬服務業原則上應適時履行告知義務，除經檢視有例外無須告知之事由外，依據資料蒐集之情形，採取適當之告知方式，以確實履行告知義務。
第十一條 殯葬服務業所屬人員利用個人資料行銷時，應明確告知當事人其所屬公司或商業名稱。 殯葬服務業首次利用個人資料行銷時，應提供當事人免付費電話、免費回郵等免費表示拒絕接受行銷之方式。 殯葬服務業利用個人資料進行行銷，當事人表示拒絕接受行銷後，應立即停止利用其個人資料繼續行銷，並周知所屬人員、受委託之公司或商業。	一、為讓當事人知曉對其進行行銷之殯葬服務業者為何，第一項規定殯葬服務業應規定所屬人員於行銷時，須確實表明業者名稱，以便讓當事人在行使拒絕接受行銷之權利時，知悉拒絕之對象為何，以免在日後追究其違法行銷責任時，發生爭議。 二、為使殯葬服務業個人資料行銷符合本法第二十條第二項及第三項規定，爰規定其應提供當事人表示拒絕接受行銷之方式及拒絕效果。
第十二條 殯葬服務業所蒐集之個人資料如需作特定目的外利用，應檢視是否符合本法第二十條第一項但書規定，得為利用之	依本法第二十條第一項規定，除本法第六條第一項規定資料外，個人資料應於蒐集之特定目的必要範圍內利用，如需

情形。	作特定目的外之利用，應符合該條項但書規定一定法定情形，爰明定殯葬服務業如需作特定目的外利用時，應先行檢視是否符合上開規定，如有違反該規定為特定目的外利用者，主管機關依本法第四十一條規定裁罰。
第十三條 殯葬服務業於當事人行使本法第三條規定之權利時，應依下列規定辦理： 一、提供聯絡窗口及聯絡方式。 二、確認是否為資料當事人之本人，或經其委託。 三、如認有本法第十條但書各款、第十一條第二項但書或第三項但書得拒絕當事人行使權利之事由，應附理由通知當事人。 四、告知是否酌收必要成本費用及其收費基準，並遵守本法第十三條處理期限規定。	依本法第三條規定，當事人就其個人資料得行使查詢、閱覽、製給複製本、補充或更正、停止蒐集、處理或利用及刪除之權利，且非公務機關除有本法第十條但書及第十一條第二項但書、第三項但書規定之情形，應於本法第十三條規定期間內准駁當事人之請求，爰規定殯葬服務業應採取之方式，以供資料當事人行使權利。
第十四條 殯葬服務業應訂定應變機制，在發生個人資料被竊取、洩漏、竄改或其他侵害事故時，迅速處理以保護當事人之權益。 前項應變機制，應包括下列事項： 一、採取適當之措施以控制事故對當事人造成損害。 二、查明事故發生原因及損害狀況，並以適當方式通知當事人。 三、研議改進措施，避免類似事故再度發生。	本法第十二條規定，非公務機關所持有之個人資料發生被竊取、洩漏、竄改或其他侵害事故者，應查明後以適當方式通知當事人，爰規定殯葬服務業在計畫中應訂定應變機制及其必要作為之相關事項，在發生資料外洩等意外事故時，得迅速遵循處理，以保護當事人之權益。
第十五條 殯葬服務業對所保有之個人資料檔案，應採取必要適當之安全設備或防護措施。 前項安全設備或防護措施應包含下列事項： 一、紙本資料檔案之安全保護設施及管理程序。 二、電子資料檔案存放之電腦、自動化機器相關設備、可攜式設備或儲存媒體，配置安全防護系統或加密機制。 三、個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片或其他存放媒介物需報廢汰換或轉作其他用途時，應採取適當防範措施，避	為確保殯葬服務業所保管之個人資料檔案不被竊取、竄改、毀損、滅失或洩漏，爰規定業者應採取必要且適當之安全設備或防護措施。

免洩漏個人資料；若委託他人執行上開行為時，殯葬服務業應對受託人為適當之監督，並明確約定相關監督事項與方式。	
第十六條 殯葬服務業為確實保護個人資料之安全，應對其所屬人員採取下列措施： 一、依據業務作業需要，建立管理機制，設定所屬人員不同之權限，並定期確認權限內容之適當性及必要性。 二、檢視各相關業務之性質，規範個人資料蒐集、處理及利用等流程之負責人員。 三、要求所屬人員妥善保管個人資料之儲存媒介物，並約定保管及保密義務。 四、所屬人員離職時取消其識別碼，並應要求將執行業務所持有之個人資料辦理交接，不得攜離在外繼續使用，並應簽訂保密切結書。	為避免殯葬服務業及其所屬人員在個人資料之保管與處理上發生弊端，導致侵害當事人權益情事，爰規定殯葬服務業為確實保護個人資料之安全，應對其所屬人員採取適當措施。
第十七條 殯葬服務業應訂定個人資料檔案安全維護查核機制，定期或不定期檢查計畫之執行情形。 前項定期檢查計畫之執行，每二年至少一次，並作成報告，其保存期限至少五年。	為確保個人資料維護安全措施發生效能，爰規定殯葬服務業應訂定個人資料檔案安全維護查核機制，定期或不定期檢查計畫之執行情形作成報告，並至少保存五年。
第十八條 殯葬服務業應留存個人資料使用紀錄、自動化機器設備之軌跡資料或其他相關之證據資料。	明定殯葬服務業應留存相關軌跡或證據資料。
第十九條 殯葬服務業業務終止後，其保有之個人資料不得繼續使用，應依下列方式處理，並留存相關紀錄，其保存期限至少五年： 一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。 二、移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。 三、其他刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。	殯葬服務業因解散、停業、歇業或其他原因終止業務後，自不得繼續使用個人資料檔案，並應作妥善處置，爰規定終止業務之殯葬服務業，應視其終止業務之原因，將所保有之個人資料予以銷毀、移轉、刪除或其他停止處理或利用等方式處理。
第二十條 殯葬服務業對於個人資料蒐集、處理及利用須符合本法第十九條及第二十條相關規定，並定期或不定期對於所屬人員施以基礎認知宣導或專業教育訓練，使	明定殯葬服務業應定期對所屬人員施以宣導或訓練講習，以使所屬人員能充分認知個人資料保護相關法令及責任範圍，避免發生違法情事。

其明瞭個人資料保護相關法令規定、責任範圍及應遵守之相關管理措施。	
第二十一條 直轄市、縣（市）主管機關應將殯葬服務業辦理個人資料檔案安全維護管理事項納入評鑑項目。	按殯葬管理條例第五十八條規定：「直轄市、縣（市）主管機關對殯葬服務業應定期實施評鑑，經評鑑成績優良者，應予獎勵。前項評鑑及獎勵之自治法規，由直轄市、縣（市）主管機關定之。」為督促殯葬服務業辦理個人資料安全維護管理事項，爰規定納入直轄市、縣（市）主管機關定期辦理殯葬服務業評鑑項目。
第二十二條 本辦法自發布日施行。	明定本辦法之施行日期。